Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 1, pp. 215–228
DOI : 10.47974/JDMSC-2411

Chaotic image encryption using circular shift and modular arithmetic

R. Amutha
Department of Electronics and Communication Engineering
Sri Sivasubramaniya Nadar College of Engineering
Kalavakkam 603110
Tamil Nadu
India

Abstract

In this paper, an image encryption algorithm using a proposed cosine chaotic map is designed. The proposed image encryption algorithm uses two levels of permutation and three levels of diffusion. The first level of permutation is done using chaotic index sequence. Second level of permutation is carried out using transformation matrix. Transformation matrix is generated using the index sequence generated by the proposed map. Modular arithmetic is used for the first level diffusion. Second level diffusion are carried out using chaotic controlled circular shift. Row and column diffusion using XOR operation is done as the third level of diffusion. The performance metrices local entropy, global entropy, chi-square, correlation coefficient, NPCR, UACI, PSNR, MSE, key space are computed for different test images. Wide chaotic region of the proposed map and large key space are verified through simulations.

Subject Classification: *94A08, 68P25, 34C23.*

Keywords: *Chaotic map, Circular shift, Confusion, Modulo diffusion, Image encryption, Cipher image.*

1. Introduction

With the widespread use of digital imaging technologies and the internet, ensuring the confidentiality and integrity of images has become paramount. Encryption techniques employ sophisticated algorithms to transform images into unreadable formats, protecting them from interception and unauthorized viewing. Advances in encryption methods, including hybrid approaches and

ORCID-ID: 0009-0009-8820-1512

E-mail: amuthar@ssn.edu.in

chaos-based techniques, continue to evolve to meet the challenges posed by increasingly sophisticated cyber threats. Effective image encryption ensures secure transmission and storage, supporting privacy and compliance requirements across various sectors. Encryption is essential in various domains, such as military communications, healthcare etc, where confidentiality and integrity of images are paramount. Motivated by the need for image encryption, the researchers developed image encryption techniques. Liu and Xia introduced a 2-D fractional-order discrete chaotic map for image encryption applications. Security is enhanced by introducing fractional-order dynamics, offering increased complexity and unpredictability in encryption operations [1]. Ponuma et al. present a compressive sensing framework for image compression and encryption [2]. Hasheminejad and Rostami proposed a a bit level multi phase encryption using Piecewise Linear Chaotic Map (PWLCM). This algorithm uses PWLCM's chaotic dynamics to achieve effective encryption of image [3]. Charif and Guennoun developed an image encryption algorithm based on chaotic billiards dynamics. Permutaion and diffusion were performed using the pseudo-random sequences generated by a two dimensional chaotic map. From the simulation result it is proved that this algorithm is resistance to common cryptographic attacks, including statistical and differential attack [4] Ponuma and Amutha developed an encryption which combines compressive sensing and chaotic systems [5].

Ponuma and Amutha proposed sparse coding based encryption technique. This method exploits the sparsity in images for efficient encryption and decryption [6]. Wang et al. developed an algorithm utilizing a chaotic model with modular sine arithmetic. This method enhances security by integrating chaotic dynamics and modular arithmetic operations, selectively encrypting specific parts of an image [9]. Hanis and Amutha presented an encryption method using an extended logistic map. Their method leverages the chaotic properties of the map to improve the security [10]. Subhashini and Amutha developed DNA based image encryption algorithm [14].

Bourekouche, Belkacem, and Messaoudi, [17] proposed a hybrid pseudo-random number generator called NLFSR-LM, which XORs outputs from an 8-bit nonlinear feedback shift register with a logistic chaotic map to improve randomness for cryptographic use. Paliwal et al. [18] developed an image encryption algorithm with a key generated from a chaotic map. The proposed algorithm uses both confusion and diffusion to enhance the security.

2. Preliminaries

2.1 *Chaotic map*

The logistic map is represented mathematically by equation (1).

$$X_{n+1} = \mu X_n(1 - X_n) \tag{1}$$

where $X \in [0,1]$ and $\mu \in [0,4]$. The chaotic range is of this map is small and is controlled by μ. Modified logistic map which has a wide chaotic range is represented mathematically as

$$X_{n+1} = mod\left(abs\left(\mu * \left(1 - \frac{\mu}{X_n}\right)(1-\mu^2)\right), 1\right) \tag{2}$$

The proposed cosine map uses modified logistic map as the seed map. The cosine chaotic map is given by the Eq. (3)

$$X_{n+1} = cos\left(2^{\left(k+mod\left(\mu*\left(1-\frac{\mu}{X_n}\right)*\left(1-\mu^2\right)\right),1\right)}\right) \tag{3}$$

where $k \in [10,24], X \in [0,1]$ and $\mu \in [0,100]$. Bifurcation plot of the proposed cosine map for $k = 15$ is depicted in Figure 1 which has a large chaotic range.

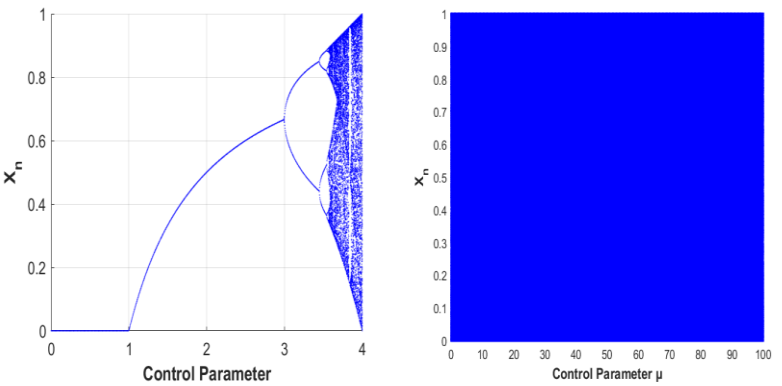


Figure 1

Bifurcation plot of a) Logistic b) Proposed.

2.2 *Lyapunov Exponent*

The Lyapunov exponent of a chaotic map quantifies the average rate at which nearby trajectories diverge, reflecting the system's sensitivity to initial conditions. A positive value indicates chaos, where small differences in starting points lead to exponential separation, characterizing the chaotic range of behaviour. This measure is crucial for understanding the unpredictability and complexity inherent in chaotic systems.

$$L = \lim_{N\to\infty}\left\{\frac{1}{N}\sum_{j=0}^{N-1}\ln|f'(X_n)|\right\} \tag{4}$$

where $f(X_n)$ is a chaotic system and $f'(X_n)$ the derivate in Eq. (4). Lyapunov Exponent values of the logistic, modified logistic and the cosine map are presented in Table 1.

Table 1
Comparison of Lyapunov exponent

μ, X_0	Lyapunov Exponent		
	Proposed cosine	Logistic	Modified Logistic
3.89429, 0.55427	16.413	0.49988	6.09885
3.91429, 0.65863	13.066	0.511	7.352

3. Proposed Method

The proposed encryption technique is represented as a block diagram in Figure 2. Two levels of permutation and three levels of diffusion is used in proposed method. The proposed method uses the following steps.

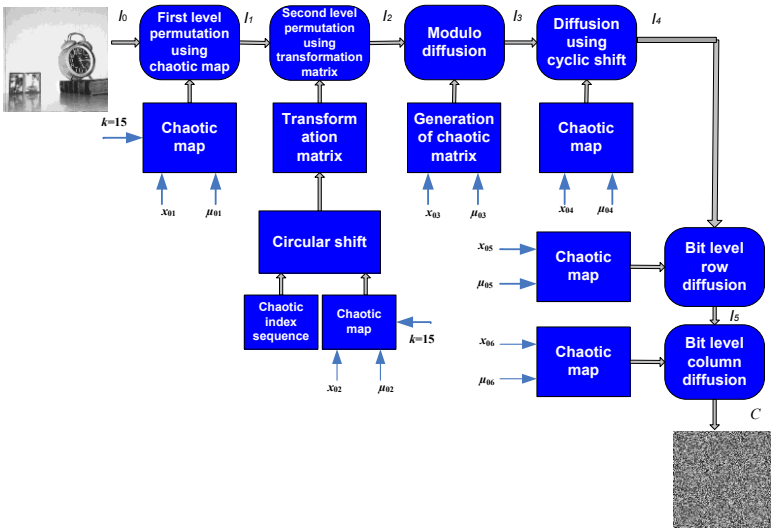


Figure 2
Proposed image encryption

Step 1: Permutation using chaotic sequence

Chaotic sequence x_1 of size $100 + MN$ is generated using Eq. (3). The first hundred values are neglected. Sequence x_1 is arranged in the ascending order and the index sequence q_1 is generated. Image I_0 is permuted using q_1 to generate the first level permuted image I_1.

Step 2: Permutation using transformation matrix

Second chaotic sequence x_2 of size $100 + MN$ is generated using Eq. (3). The index sequence q_2 is generated by sorting x_2 in ascending order, after

neglecting the first 100 values. A sequence s_2 of size 256 is generated using Eq. (5).

$$s_2 = mod(floor(x_2 * 10^{16}), 10) \tag{5}$$

The sequence q_2 is shifted to the right circularly using the first value present in s_2. The circularly shifted sequence is the first row of the transformation matrix. Similarly, the second row of the transformation matrix is generated by circularly shifting the index sequence q_2 by the second value present in s_2. Repeating the same process, the transformation matrix T of size 256*256 is generated. I_1 is permuted using the transformation matrix T to generate the image I_2.

Step 3: Diffusion by modular operation

Third sequence x_3 of size $100 + MN$ is generated using Eq. (3). The sequence is quantized using the Eq. (6) and represented as a matrix T_2 of order $M * N$. Modulo 256 addition of the matrix T_2, I_2 is carried out to get T_3. Transpose the matrix T_3 to get diffused image I_3.

$$T_1 = mod(floor(x_3 * 10^{16}), 256) \tag{6}$$

Step 4: Diffusion using chaotic control circular shift

Fourth chaotic sequence x_4 of size $100 + MN$ is generated and quantized using Eq. (7) to obtain s_3.

$$s_3 = mod(floor(x_4 * 10^{16}), 8) \tag{7}$$

Each pixel in the image $I_3$is converted into binary. The bits in each pixel is circularly shifted to the right. The number of shifts is controlled by the sequence s_3 to get diffused image I_4.

Step 5: Row diffusion

A chaotic sequence x_5 of size $100 + M$ is generated using Eq. (3). The sequence x_5 is quantized using Eq. (8).

$$s_4 = mod(floor(x_5 * 10^{16}), 256) \tag{8}$$

XOR operation is used for row diffusion. The diffusion operation is represented mathematically by Eq. (9).

$$I_6 = \begin{cases} s_4 + I_5(i) & i=1 \\ I_6(i-1) + I_5(i) & i=2,3,\ldots,M \end{cases} \tag{9}$$

Step 6: To further improve the diffusion, column diffusion is carried similar to the row diffusion. A chaotic sequence x_6, of size $100 + N$ is generated using Eq. (3). A sequence s_5 is generated using Eq. (10) by quantizing the chaotic sequence x_6.

$$s_5 = mod(floor(x_6 * 10^{16}), 256) \tag{10}$$

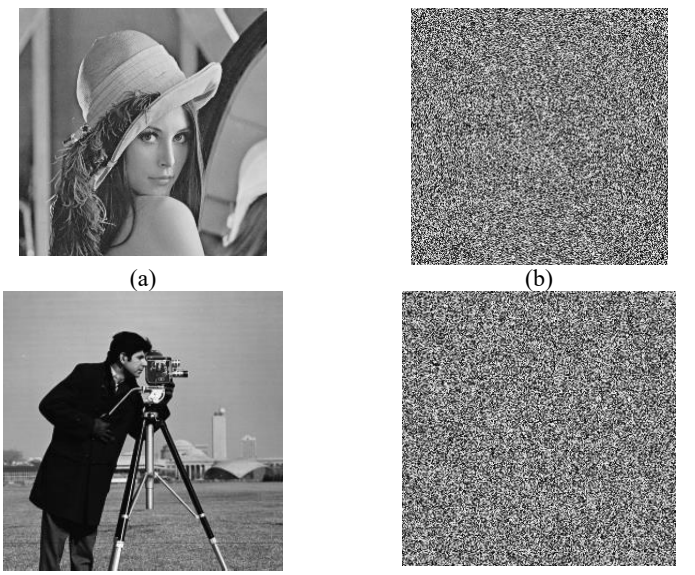
The column diffusion is done by using equation (11)

$$C = \begin{cases} s_5 + I_6(i) & i=1 \\ C(i-1) + I_6(i) & i=2,3,\ldots,N \end{cases} \quad (11)$$

The output of the column diffusion is the encrypted image C.

4. Performance analysis

Simulations are carried using the grayscale test images from SIPI database. The proposed algorithm is tested using Lena and Cameramen images. Original and cipher images is depicted in Figure 3. By comparing the Figure, a, c with b and d it is evident that the algorithm convert test images into a non- meaningful cipher image.



(a) (b)

(c) (d)

Figure 3
Plain Image: (a) Lena (c) Cameraman, Cipher Image: (b) Lena cipher (d) Cameraman cipher

4.1 *Statistical Analysis*

Statistical analysis of image encryption evaluates the effectiveness of algorithms in obscuring patterns and enhancing security. Various test such as histogram analysis, entropy measurement, and correlation coefficient assessment are done to ensure robustness against attacks.

4.1.1 Histogram Analysis

Histogram represents the distribution of pixels. Histogram of the lena and cameraman and their corresponding cipher images are dipicted in Figure 4. The

histogram of the cipher image is evenly distributed and hence our work is robust against attacks.

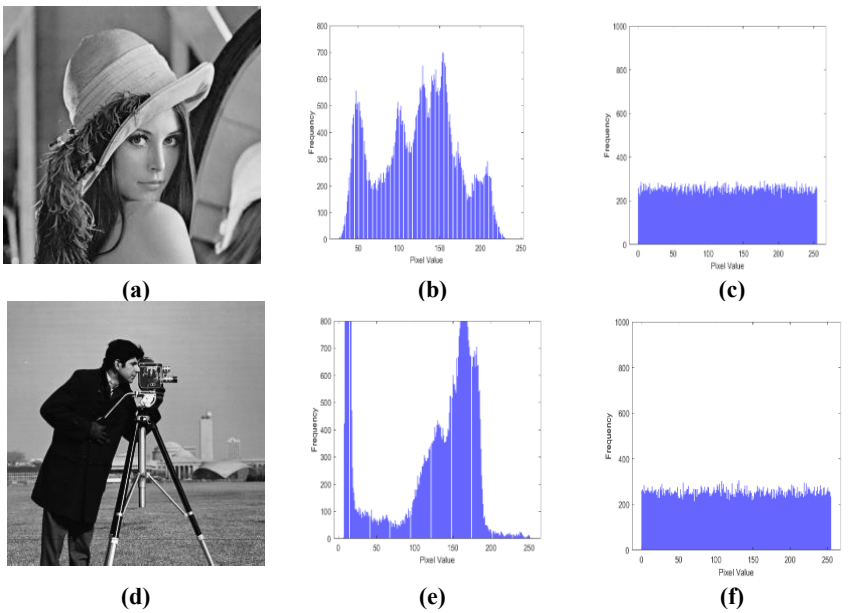


Figure 4
Plain image: (a) Lena (d) Cameraman, Histogram: (b) Lena (e) Cameraman, Histogram of cipher: (c) Lena (f) Cameraman

4.1.2 Chi-Square test

The chi-square test for image encryption assesses the uniformity of pixel distribution in the encrypted image by comparing observed and expected frequencies. The chi-square test is performed for various test images using Eq. (12) and listed in Table 2. Chi- square value of our work is lesser than the critical value 293.2478. A low chi-square value indicates that there is no leakage of information from cipher image and hence enhancing its security against attacks.

$$\chi^2 = \sum_{i=0}^{255} \frac{(d-e)^2}{e} \tag{12}$$

where 'd' is the count of each gray value that has occurred in the cipher image and 'e' is given by

$$e = \frac{M * N}{256}$$

where M and N is the dimension of the image.

Table 2
Comparison of Chi-square value

Test Images 256x256	Proposed method	Xian et al. (2020) [7]	Wang et al. (2021) [8]
5.1.10	237.4844	263.09	259.4766
5.1.11	218.2031	247.44	249.9297
5.1.12	228.4531	236.38	288.4219
5.1.14	257.6563	275.89	256.4297

4.1.3 Correlation Analysis

It is crucial to prevent high connectivity between neighbouring pixels in the encrypted image. Attackers frequently calculate the correlation between neighbouring values, and high value reveal information about the image, compromising its security. Results of the correlation in horizontal (H), vertical (V), and diagonal (D) directions are depicted in Figure 5. The correlation coefficient (CC) of the various test and its cipher images are computed using Eq. (13) and depicted in Table 3. It is evident from Table 3 that the CC of the cipher image is approximately equal to zero.

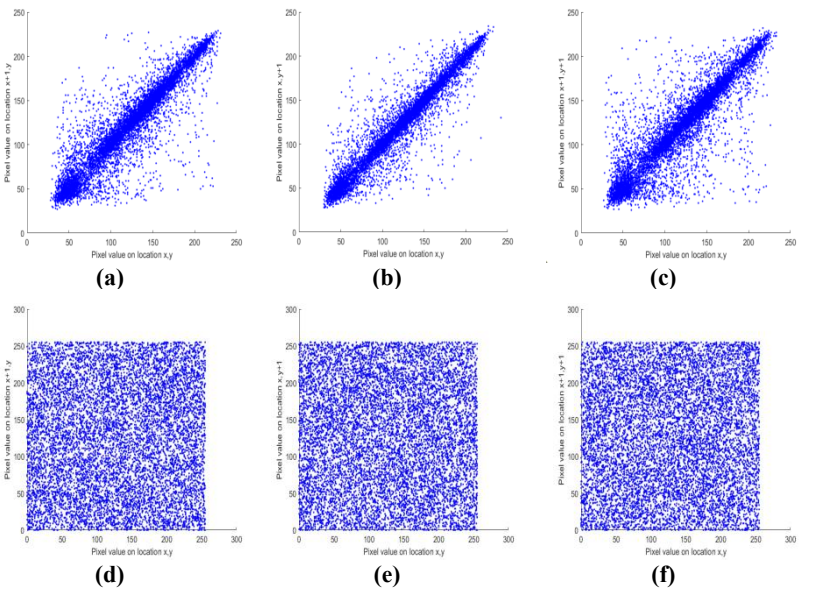


Figure 5
Pixel correlation plot of test image Lena: a horizontal, b vertical, c diagonal. Pixel correlation plot of cipher image Lena: d horizontal, e vertical, f diagonal

$$R_{xy} = \frac{cov(v,x)}{\sqrt{C(v)C(x)}} \tag{13}$$

where

$$cov(v,x) = \frac{1}{N}\sum_{j=1}^{N}(v_j - E(v))(x_j - E(x))$$

$$C(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N} x_j$$

Table 3

Comparison of Correlation Coefficient

Test Image 256x256	CC	Original image	Encrypted image	Wang et al. (2021) [8]	Alawida (2023) [11]
5.1.10	H	0.9035	0.0053	0.0044	−0.007
	V	0.8597	-0.0047	- 0.0006	0.0017
	D	0.8234	-0.0020	- 0.0052	0.0004
5.1.11	H	0.9588	0.0018	0.0004	0.0144
	V	0.9383	0.0004	-0.0019	−0.0003
	D	0.8843	-0.0036	- 0.0049	0.0009
5.1.12	H	0.9568	-0.0008	0.0067	0.0174
	V	0.9730	-0.0092	- 0.0002	0.00012
	D	0.9377	0.0126	- 0.0055	0.0001

4.1.4 Global Entropy Analysis

Entropy test evaluates the randomness and unpredictability of pixels in cipher image. Global entropy of three test and its cipher images are evaluated using Eq. (14) and presented in Table 4.

$$H = \sum_{i=0}^{255} p(m_i) log_2 \frac{1}{p(m_i)} \tag{14}$$

$p(m_i)$ is the probability of the image pixels. From Table 4 it is observed that the global entropy value of the cipher image is close to expected value of 8 and comparable with [8, 12]. Entropy of the cipher image is higher than its original image indicating the effectiveness of the proposed algorithm.

Table 4

Global Entropy values

Test Image 256x256	Global Entropy of Plain Image	Proposed Method	Global Entropy of Cipher Image	
			Wang et al. (2021) [8]	Wen et al. (2023) [12]
5.1.10	7.3118	7.9974	7.9973	7.9975
5.1.11	6.4523	7.9976	7.9970	7.9971
5.1.12	6.7057	7.9975	7.9975	7.9962

Local Shannon entropy measures the unpredictability and randomness within a specific region of an encrypted image, indicating the strength of the encryption. High local Shannon entropy ensures that even small sections of the image exhibit high randomness, contributing to the overall security of the encryption scheme. Local Shannon entropy is computed using Eq. (15) and depicted in Table 5**.** Local Shannon entropy of our method is comparable with that of [11, 16].

$$H_{s,TB}(G) = \sum_{i=1}^{s} \frac{H(G_i)}{s} \tag{15}$$

where $H(G_i)$ is the Shannon entropy of randomly selected block of cipher image.

Table 5

Local Shannon Entropy values

Test Image 256x256	Proposed method	Alawida (2023) [11]	Wang et al. (2024) [16]
5.1.11	7.9034	7.9034	7.9019
5.1.12	7.9028	7.9033	7.9042

4.1.5 MSE and PSNR Analysis

MSE and PSNR are computed using the Eq. (16) and (17) and presented in Table 6.

$$MSE = \frac{1}{M*N} \sum_{u=1}^{M} \sum_{v=1}^{N} (P(u,v) - C(u,v))^2 \tag{16}$$

$P(u,v)$ and $C(u,v)$ are the individual pixels of plain and cipher images respectively.

$$PSNR = 10 * log_{10}\left(\frac{255^2}{MSE}\right) \tag{17}$$

From the Table 6A and 6B, it is observed that the PSNR and MSE values of the proposed method is comparable with that of [12, 15].

Table 6A

PSNR values

Test Image 256x256	PSNR (dB)		
	Proposed Method	Wen et al. (2023) [12]	Wen et al. (2024) [15]
5.1.10	9.3089	9.2858	9.2692
5.1.11	7.7409	7.7187	7.7554
5.1.12	7.3	7.2913	7.2710
5.1.14	9.2546	9.2311	9.2195

Table 6B

MSE values

Test Image 256x256	MSE		
	Proposed Method	Wen et al. (2023) [12]	Wen et al. (2024) [15]
5.1.10	7624.19	7664.70	7694.17
5.1.11	10939.42	10995	10902.98
5.1.12	12108.13	12133	12189.26
5.1.14	7720.03	7762	7782.77

The local entropy, global entropy, chi-square, MSE, PSNR are computed for the proposed image encryption algorithm and tabulated in Table 7.

Table 7

Results for encrypted images

Test Image 256x256	Entropy of plain Image	Global Entropy of cipher Image	Local Entropy	Chi-square	MSE	PSNR (dB)
5.1.11	6.4523	7.9976	7.9034	218.2031	10939.42	7.7409
5.1.12	6.7057	7.9975	7.9028	228.4531	12108.13	7.3

4.1 *Differential Attack Analysis*

Resistance to differential attack is measured using number of pixel change rates (NPCR) and unified average changing intensity (UACI). The NPCR and UACI are computed using Eq. (18) and (19) and listed in Table 8A and 8B. NPCR and UACI value of our method is compared with [11, 16] and is greater than the critical value of 99.5693 and 33.6447 respectively [10].

$$NPCR = \frac{1}{M*N}\sum_{y,z} Difference(y,z) * 100\% \quad (18)$$

where

$$Difference(y,z) = \begin{cases} 0, Img_1(y,z) = Img_2(y,z) \\ 1, Img_1(y,z) \neq Img_2(y,z) \end{cases}$$

$$UACI = \frac{1}{M*N} \frac{\sum_{s,t} |Img_1(y,z) - Img_2(y,z)|}{255} * 100\% \quad (19)$$

Table 8A

NPCR values

Test Image 256x256	NPCR		
	Proposed method	Alawida (2023) [11]	Wang et al. (2024) [16]
5.1.09	99.6002	99.67	99.6544
5.1.10	99.6109	99.65	99.5962
5.1.11	99.6521	99.91	99.6075

Table 8B

UACI values

Test Image 256x256	UACI		
	Proposed method	Alawida (2023) [11]	Wang et al. (2024) [16]
5.1.09	33.5178	33.512	33.5564
5.1.10	33.4317	33.382	33.4531
5.1.11	33.4939	33.487	33.4505

4.3 *Key space Analysis*

Key space analysis is crucial for assessing the security of an image encryption algorithm. A larger key space makes it more difficult for an attacker to predict the correct key through brute-force attacks. To withstand exhaustive attacks, a minimum key space of $10^{32} * 10^{32} * 10^{32}$ is required. With the parameters $(X0, \mu)$ of the chaotic sequences having 16-digit precision, the key space of our encryption method is

$$10^{32} * 10^{32} * 10^{32} * 10^{32} * 10^{32} * 10^{32} = 10^{192} \approx 2^{637}$$

It is compared with existing works as shown in Table 9.

Table 9

Key Space Analysis

Proposed Method	Alawida (2023) [11]	Panwar et al. (2024) [13]
2^{637}	2^{128}	2^{128}

5. Conclusion

An image encryption algorithm using modular arithmetic is proposed. A new cosine logistic map with large chaotic region is also proposed in this work. Lyapunov exponent and bifurcation results shows that the proposed map has large chaotic region. Two level of confusion and three level of diffusion are used in the proposed method to increase the security. A large key space of 2^{637} is used in this proposed method to avoid brute force attack. Experimental results demonstrate that our method provide high level of security and resistance to various attacks.

References

[1] Z. Liu and T. Xia, "Novel two dimensional fractional-order discrete chaotic map and its application to image encryption," *Appl. Comput. Informatics,* vol. 14, no. 2, pp. 177-185 (2018) doi: 10.1016/j.aci.2017.07.002.

[2] R. Ponuma, R. Amutha, and B. Haritha, "Compressive sensing and hyper-chaos-based image compression-encryption," in Proc. 2018 Fourth Int. Conf. Adv. Electr. Electron. Inf. Commun. Bio-Informatics (AEEICB), pp. 1-5, *IEEE* (2018), doi: 10.1109/AEEICB.2018.8480989.

[3]. A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map," *Optik*, vol. 184, pp. 205-213 (2019) doi: 10.1016/j.ijleo.2019.03.065.

[4] Charif, K and Guennoun, Z. E. A, "A novel image encryption algorithm based on chaotic billiards" *Journal of Discrete Mathematical Sciences and Cryptography,* vol 24, no 1, pp. 129–154, (2019) doi: 10.1080/09720529.2019.1675302.

[5] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools Appl.*, vol. 78, pp. 11857-11881 (2019) doi: 10.1007/s11042-018-6745-3.

[6] R. Ponuma and R. Amutha, "Image encryption using sparse coding and compressive sensing," *Multidimensional Syst. Signal Process.,* vol. 30, pp. 1895-1909 (2019) doi: 10.1007/s11045-019-00634-x.

[7] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion" *Opt. Lasers Eng.,* vol. 134, (2020) Art.No. 106202. doi: 10.1016/j.optlaseng.2020.106202.

[8] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-

embedding chaotic map," *Chaos Solitons Fractals*, vol. 150, 2021) Art. No. 111117. doi: 10.1016/j.chaos.2021.111117.

[9] X. Wang, N. Guan, and P. Liu, "A selective image encryption algorithm based on a chaotic model using modular sine arithmetic," *Optik*, vol. 251, Art. No. 168955 (2022). doi: 10.1016/j.ijleo.2022.168955.

[10] H. Stanley and A. Ramachandran, "Extended logistic map for encryption of digital images" *Int. J. Nonlinear Sciences and Numerical Simulation*," vol. 23, no. 7-8, pp. 985-1000, (2022) doi: 10.1515/ijnsns-2022-0028.

[11] M. Alawida, "A novel chaos-based permutation for image encryption," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 6, Art. No. 101595 (2023). doi: 10.1016/j.jksuci.2023.101595.

[12] H. Wen, Y. Lin, Z. Xie, and T. Liu, "Chaos-based block permutation and dynamic sequence multiplexing for video encryption," *Sci. Rep.*, vol. 13, Art. No. 14721 (2023). doi: 10.1038/s41598-023-41082-9.

[13] A. Panwar, G. Biban, R. Chugh, A. Tassaddiq, and R. Alharbi, "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images," *Heliyon*, vol. 10, no. 11, Art No e31618 (2024). doi: 10.1016/j.heliyon.2024. e31618.

[14] S. Kumaran and A. Ramachandran, "Image encryption using modified perturbed logistic map, "*Int. Arab J. Inf. Technol.* (IAJIT)" vol. 21, no. 5, pp. 866-878 (2024) doi: 10.34028/iajit/21/5/8.

[15] H. Wen, Y. Lin, S. Kang, X. Zhang, and K. Zou, "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion," *iScience*, vol. 27, no. 1, Art No. 108610 (2024). doi: 10.1016/j.isci.2023.108610.

[16] Y. Wang, L. Chen, K. Yu, and H. Fang, "Multi-key spatio-temporal chaotic image encryption and retrieval scheme" *Nonlinear Dyn.,* vol. 112, no. 4, pp. 3003-3025 (2024) doi: 10.1007/s11071-023-09170-7.

[17] H. Bourekouche, S. Belkacem, and N. Messaoudi, "Efficient image encryption scheme using a nonlinear shift register and chaos" *Journal of Information and Optimization Sciences*, vol 45, no. 1, pp. 157-180 (2024) doi:10.47974/JIOS-1399

[18] M. Paliwal, P. Soni, R. Kumar, A. Goyal, M. Malik, and B. Goyal, "Chaotic map-based selective image encryption via diffusion and confusion" *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 763–773 (2024) doi: 10.47974/JDMSC-1953.

Received February, 2025